



September 7, 2006

VIA ELECTRONIC DELIVERY

Ms. Marcy Greene
Federal Communications Commission
Enforcement Bureau
445 12th Street, SW
Washington D.C. 20554

Re: CC Docket No. 96-115

Dear Ms. Greene:

Virgin Mobile USA, LLC ("Virgin Mobile") files this response to your request for additional information regarding Virgin Mobile's policies and practices for the protection of customer-sensitive information. Virgin Mobile supports and understands the need to implement policies and practices to prevent the unauthorized disclosure of personally identifiable customer information, including customer proprietary network information ("CPNI").

Safeguarding customer-sensitive information remains a top priority at Virgin Mobile and is a responsibility that Virgin Mobile takes seriously. Virgin Mobile has been an innovator in carrier security procedures since it launched its service in July 2002, and, to our knowledge, the company was the first nationwide carrier to implement a mandatory consumer-set password system (the "vKey"). The centerpiece of Virgin Mobile's security practices, the vKey system protects against the unwarranted disclosure of customer-sensitive information to unauthorized third parties. In addition to the vKey, Virgin Mobile protects customer-sensitive information through compliance with all Federal Communications Commission ("FCC" or "Commission") regulations governing the use and disclosure of CPNI, as well as internal policies governing external requests for the disclosure of customer information and records. Virgin Mobile believes that the security practices it has implemented thoroughly protect customer-sensitive information and contribute greatly to customer satisfaction and the company's success.

A. vKey System

Virgin Mobile maintains a 100-percent password-protected account management system known as the vKey. Under this regime, a customer must provide a proper Virgin Mobile phone number and associated password (the vKey) to access any customer account information. During the service activation process, Virgin Mobile requires customers to select an

alphanumeric, six-digit vKey that only the customer would know.¹ Only after a customer properly enters their telephone number and vKey can the customer access his or her account information, including a list of their most-recent calls, account balance and other personally-identifiable information. A customer also must provide his or her telephone number and vKey irrespective of whether the customer attempts to access account information online or through Virgin Mobile At Your Service, the company's customer care group.

In the event that a customer misplaces or forgets her vKey, Virgin Mobile requires the customer to answer a vKey reminder question. During the service activation process, Virgin Mobile provides customers with a pull-down menu of potential reminder questions; the answer to which only the customer would know. The customer must provide the answer to this question any time the customer forgets or misplaces their vKey. Should the customer fail to properly answer their secret question online, the customer will be denied access to the account information. For telephone requests, Virgin Mobile At Your Service customer care personnel are trained to deny access to the account in the event that a customer misplaces or forgets their vKey. In situations in which the customer does not have the vKey or the answer to their secret question, Virgin Mobile customer care personnel will permit the selection of a new vKey only if the customer provides other account information that only the customer would know. For instance the customer could provide the date and amount of their most recent account replenishment. Finally, Virgin Mobile customer personnel are continuously trained and provided with updated information regarding any changes in the company's vKey system.²

Virgin Mobile believes that the vKey system has been effective in protecting against the disclosure of customer-sensitive information to unauthorized third parties. By requiring a telephone number and vKey to access any account information, the vKey system significantly reduces the potential for the unwarranted disclosure of customer information. In addition, the user-friendly nature of the vKey system and Virgin Mobile's streamlined carrier-customer relationship model in which customers can only obtain account information online or telephonically has driven customer acceptance of the vKey.

B. Protection of CPNI

Virgin Mobile also protects its customer-sensitive information through compliance with all applicable federal and state statutes and regulations, including FCC requirements governing the protection, use and disclosure of CPNI. Virgin Mobile restricts access to CPNI and personally-identifiable customer information to only those employees and agents necessary to provide or market Virgin Mobile's services and products. Virgin Mobile also trains its employees and agents with access to CPNI on the proper use and handling of customer-sensitive information. Any Virgin Mobile employee or agent that violates the company's policies with respect to the use and disclosure of CPNI remains subject to disciplinary procedures, including termination of employment. Finally, all vendors that obtain any CPNI or personally-identifiable

¹ Virgin Mobile advises its customers not to share their vKey with any other individual for any reason. Customers may change their vKey at any time either online or through the Virgin Mobile customer hotline.

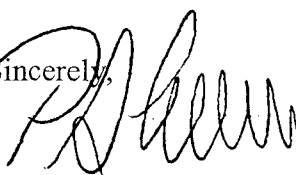
² Additional information regarding Virgin Mobile's vKey system can be obtained at www.virginmobileusa.com.

customer information are contractually bound to keep all such information confidential, use such information only to provide services to the company and immediately disclose any security breach regarding such information to Virgin Mobile.

C. External Requests for Information

Virgin Mobile has established a rigorous internal policy governing external requests for customer-sensitive information to guard against the unwarranted disclosure of this information. This policy sets forth the procedures by which Virgin Mobile personnel must respond to requests for access to and the production of customer-sensitive information from: (1) current Virgin Mobile customers, (2) law enforcement agencies, and (3) third-party, non-governmental individuals (e.g., relatives, third-party attorneys, etc.). The policy details the form of authorization required and a description of the procedures that company personnel must follow to ensure that any disclosure of customer-sensitive information is undertaken pursuant to the company's obligations under current law. By establishing clear and coherent procedures for the disclosure of customer-sensitive information, this policy ensures the consistent protection of CPNI and other customer-sensitive information and documentation. Finally, Virgin Mobile trains company personnel in accordance with this policy, and all employees must annually verify their familiarity with the procedures set forth therein.

Virgin Mobile applauds the Commission's attention to issues relating to the protection of customer-sensitive information. Virgin Mobile understands the need to protect customer information from disclosure to unauthorized third parties. Virgin Mobile believes that the practices it has implemented, including the vKey system, thoroughly protect its customers' personally identifiable information from unwarranted disclosure. Finally, Virgin Mobile would be pleased to arrange a live demonstration of the company's security practices, including its vKey system, for the Commission.

Sincerely,


Peter Lurie
General Counsel
Virgin Mobile USA, LLC
10 Independence Blvd
Warren, NJ 07059
908/607-4017